RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: HT-R06

PROTECTED: The 6th Annual Report from the SOC at RSAC

Cary Wright
VP Product Management
Endace
linkedin.com/in/caryw

Jessica Oppenheimer
Director, Security Operations
Cisco Systems
linkedin.com/in/jessbair

Steve Fink
CTO/CISO
Secure Yeti
linkedin.com/in/infosecfink

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

104-105
RSAC 2025 Conference
3 Materials Pickup
RSAC 2025 Conference
Many Voices. One Community.
Wireless Internet
Connect to SSID: .RSACONFERENCE
(Subject to the Wireless Policy)
Free wireless available in select Conference areas. The wireless network available at the Moscone Center is an open, unsecured 5 GHz network.
Important! Cisco Systems and Endace will be using data from the Moscone Wireless Network to provide Security Operations Center services. We strongly recommend that you use appropriate security measures, such as utilizing a VPN connection, installing a personal firewall, and keeping your operating system and software up-to-date with security patches. We recommend turning off your wireless adapter when not in use and ensuring ad-hoc (peer-to-peer) capabilities are disabled on your device.
#RSAC
blackhat
ATTENTION

The SOC Team

- 5 Endace Analysts
- 9 Cisco/ Splunk Analysts
- 3 Threat Hunters
- 3 Managers

The SOC at RSAC Conference

- Since RSAC 2017
- 9 Public Tours: 20-50 people
- Multiple Press Interviews
- Annual Findings Report

- Conference SPAN/TAP
- Cisco Catalyst Switch
- EndaceProbe
  - Packet Capture
  - Log Gen and File Extraction
- Splunk Cloud integrations

- Splunk Enterprise Security
- Cisco Secure Firewall – Intrusion Detection
- Cisco Security Cloud
  - Cisco Breach Protection Suite
  - Cisco Cloud Protection Suite
  - Cisco User Protection Suite

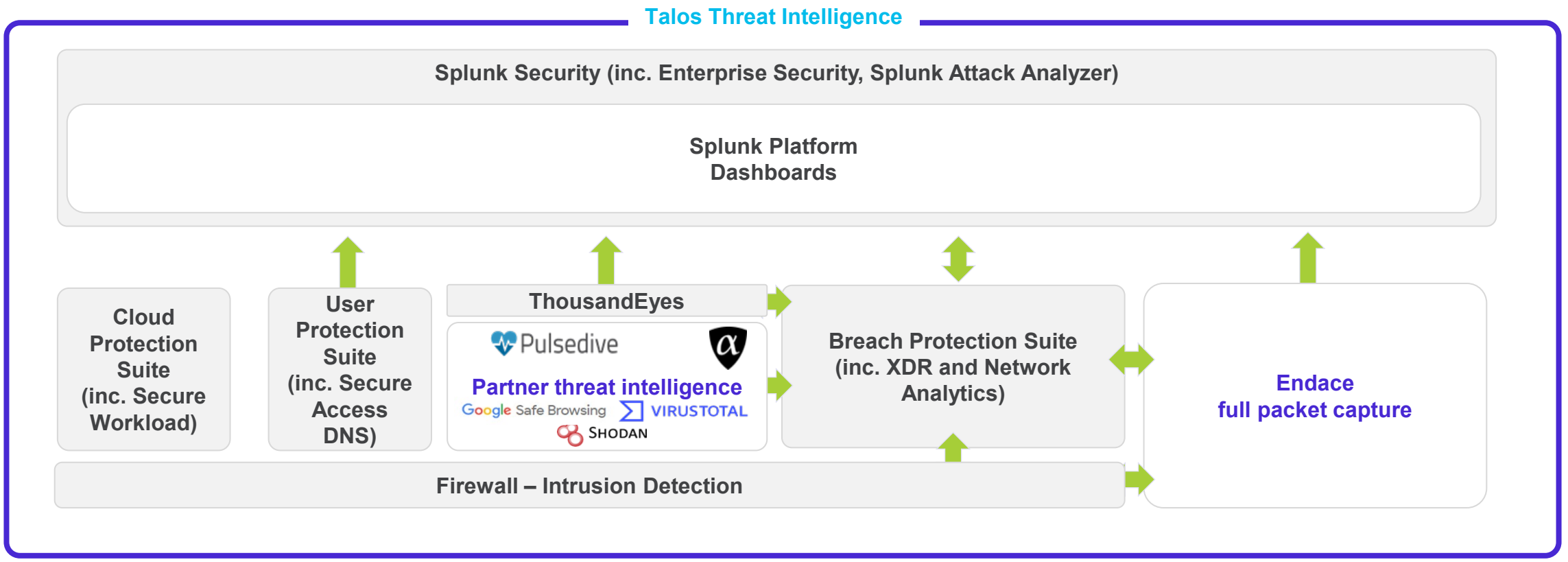
- alphaMountain.ai
- Pulsedive
- Cisco Talos
- Open source threat intel

cisco

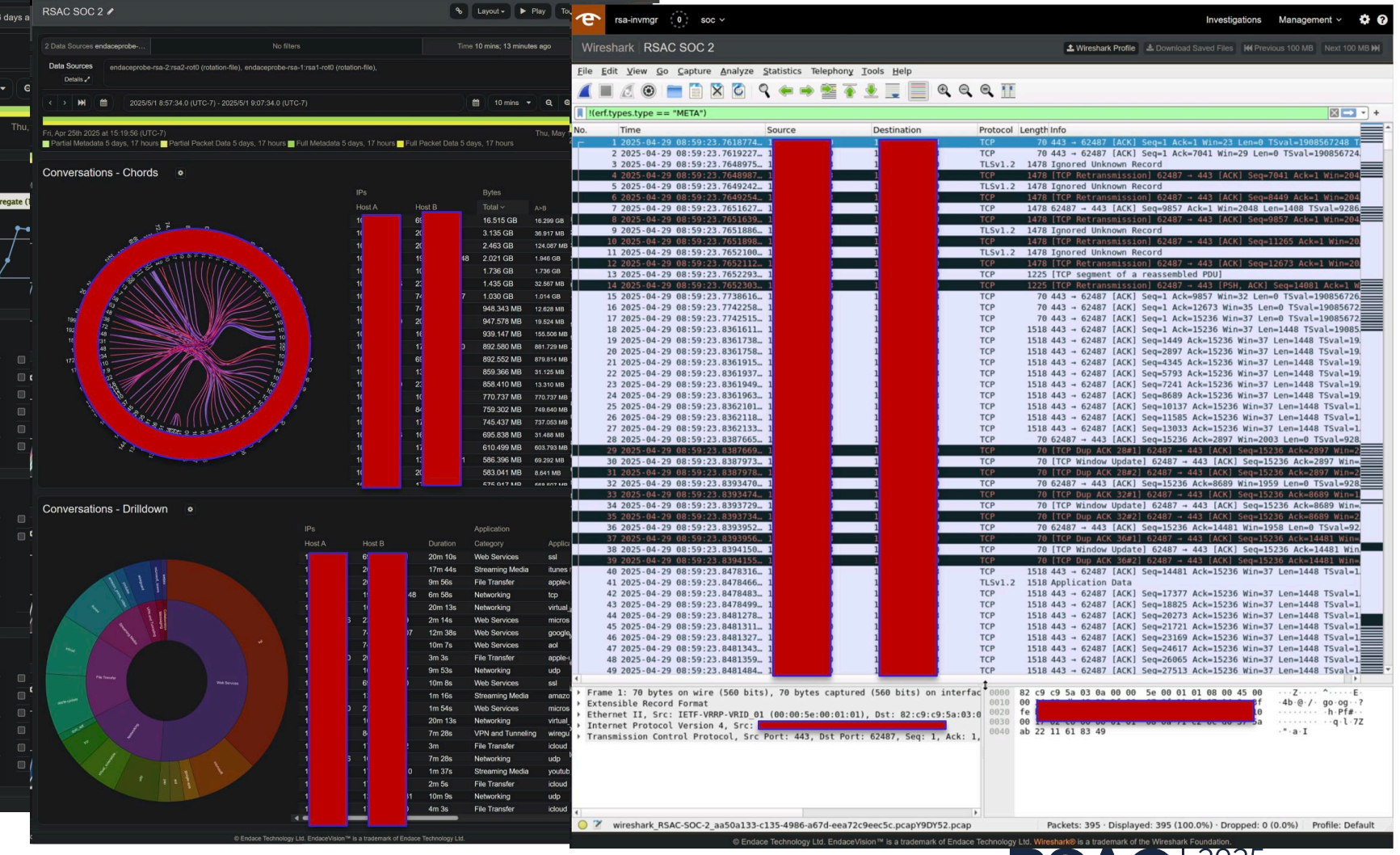
endace
Record. Respond.

RSAC 2025 Conference

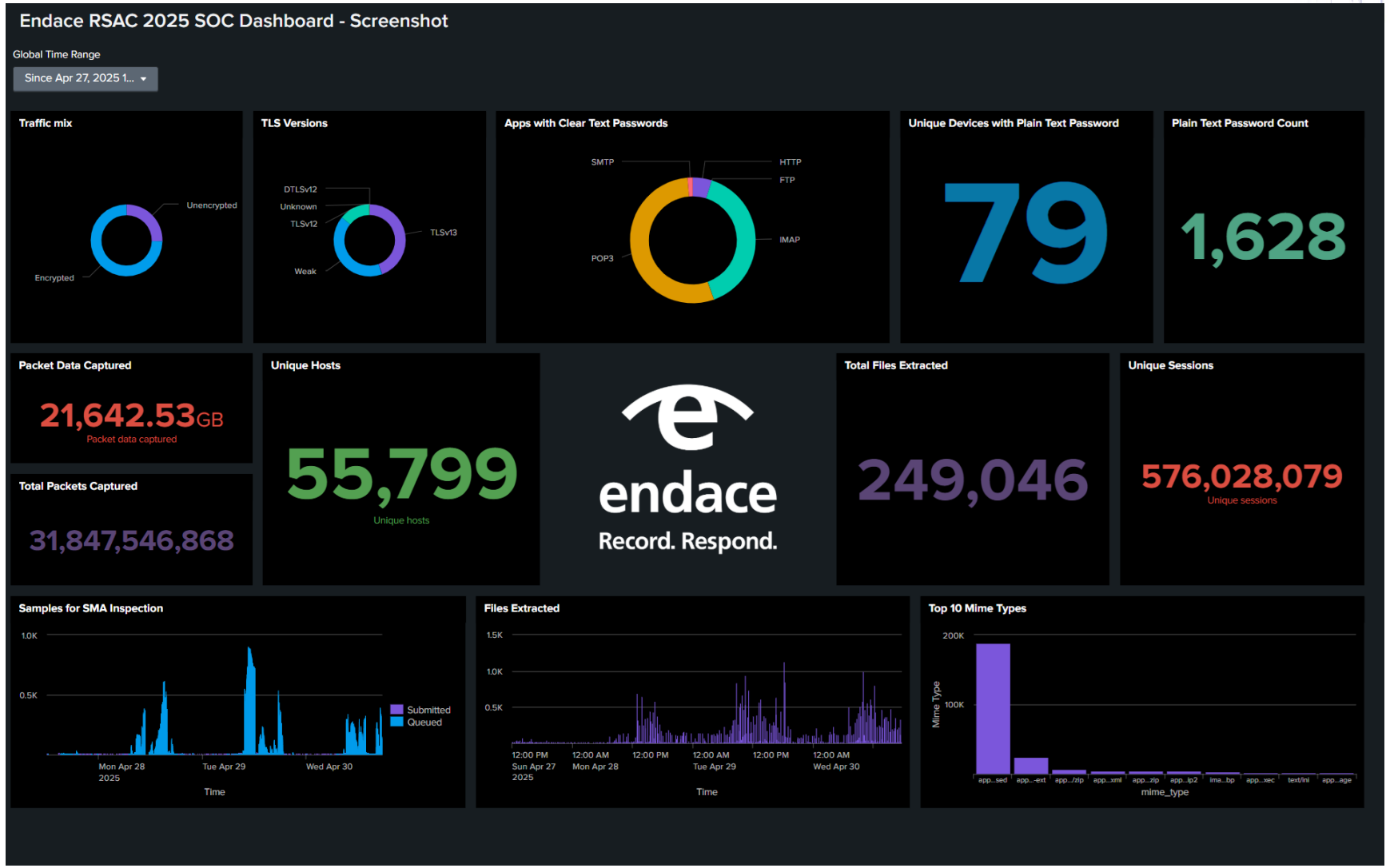
SOC Architecture



Endace SOC Dashboards Journey


rsa-invmgr
soc
Investigations
Management
Wireshark | RSAC SOC 2
Wireshark Profile
Download Saved Files
Previous 100 MB
Next 100 MB
File Edit View Go Capture Analyze Statistics Telephony Tools Help
!(erf.types.type == "META")
No.
Time
Source
Destination
Protocol
Length
Info
Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interfac
Extensible Record Format
Ethernet II, Src: IETF-VRRP-VRID_01 (00:00:5e:00:01:01), Dst: 82:c9:c9:5a:03:0
Internet Protocol Version 4, Src:
Transmission Control Protocol, Src Port: 443, Dst Port: 62487, Seq: 1, Ack: 1,
wireshark_RSAC-SOC-2_aa50a133-c135-4986-a67d-eea72c9eec5c.pcapY9DY52.pcap
Packets: 395 · Displayed: 395 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
© Endace Technology Ltd. EndaceVision™ is a trademark of Endace Technology Ltd. Wireshark® is a trademark of the Wireshark Foundation.

Endace SOC Dashboards Journey



Files Journey - Integrations Advantage

"Captain's log, Stardate 41153.7. Our destination is the Malware Analytics…" a file journey description. How the SOC keep the file monitored

40,000,000,000+ Packets Captured

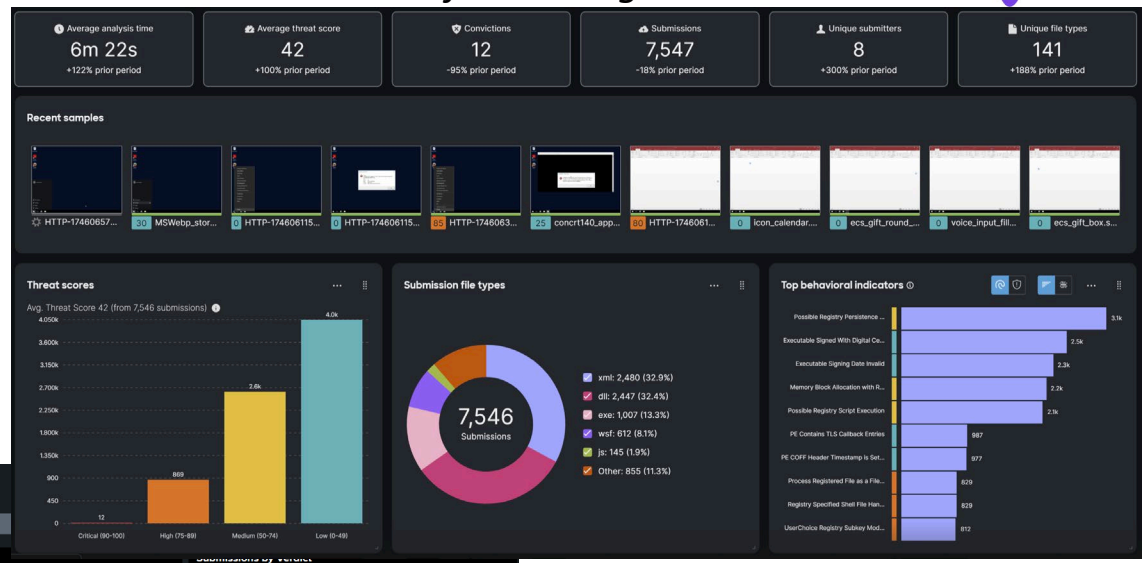
endace Record. Respond.

270,000+ files Extracted

Pivot back to Endace PCAP to Investigate

26,374 files sent to Splunk Attack Analyzer

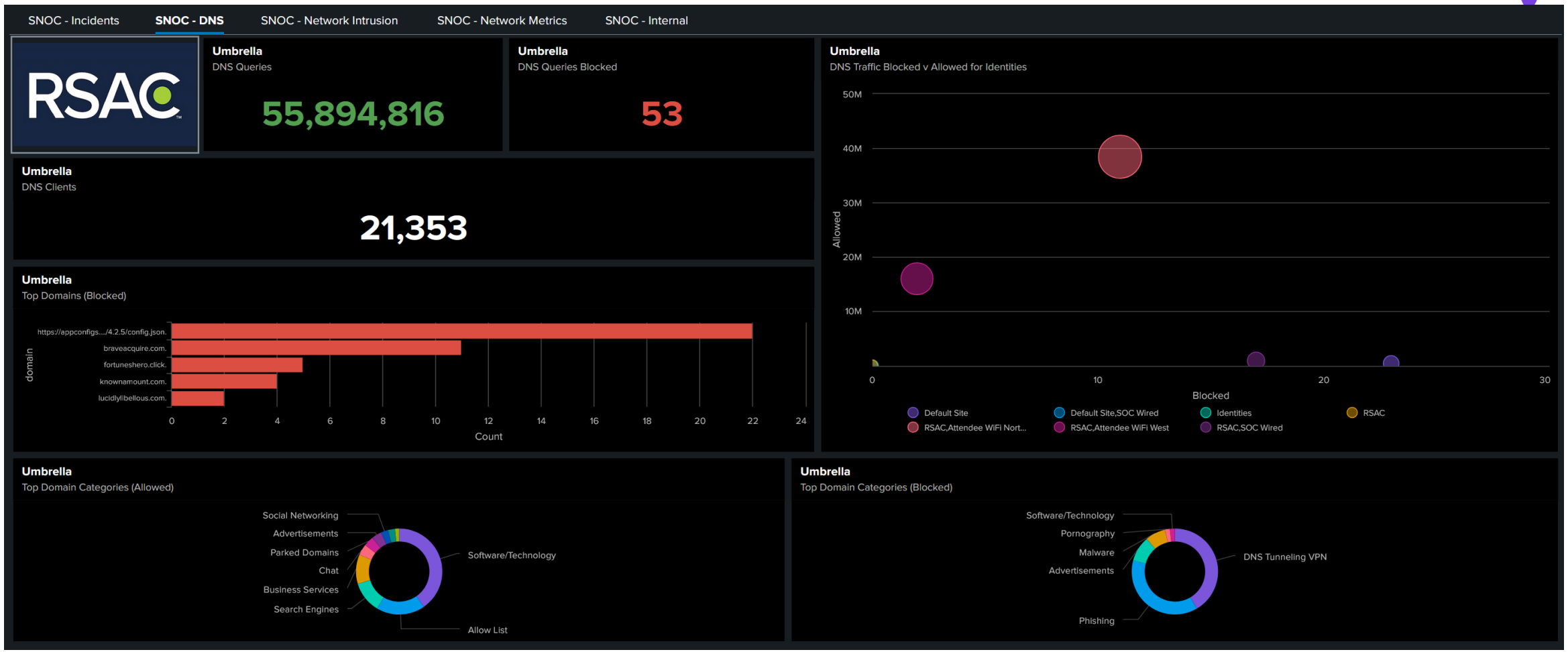
Detections for Investigation



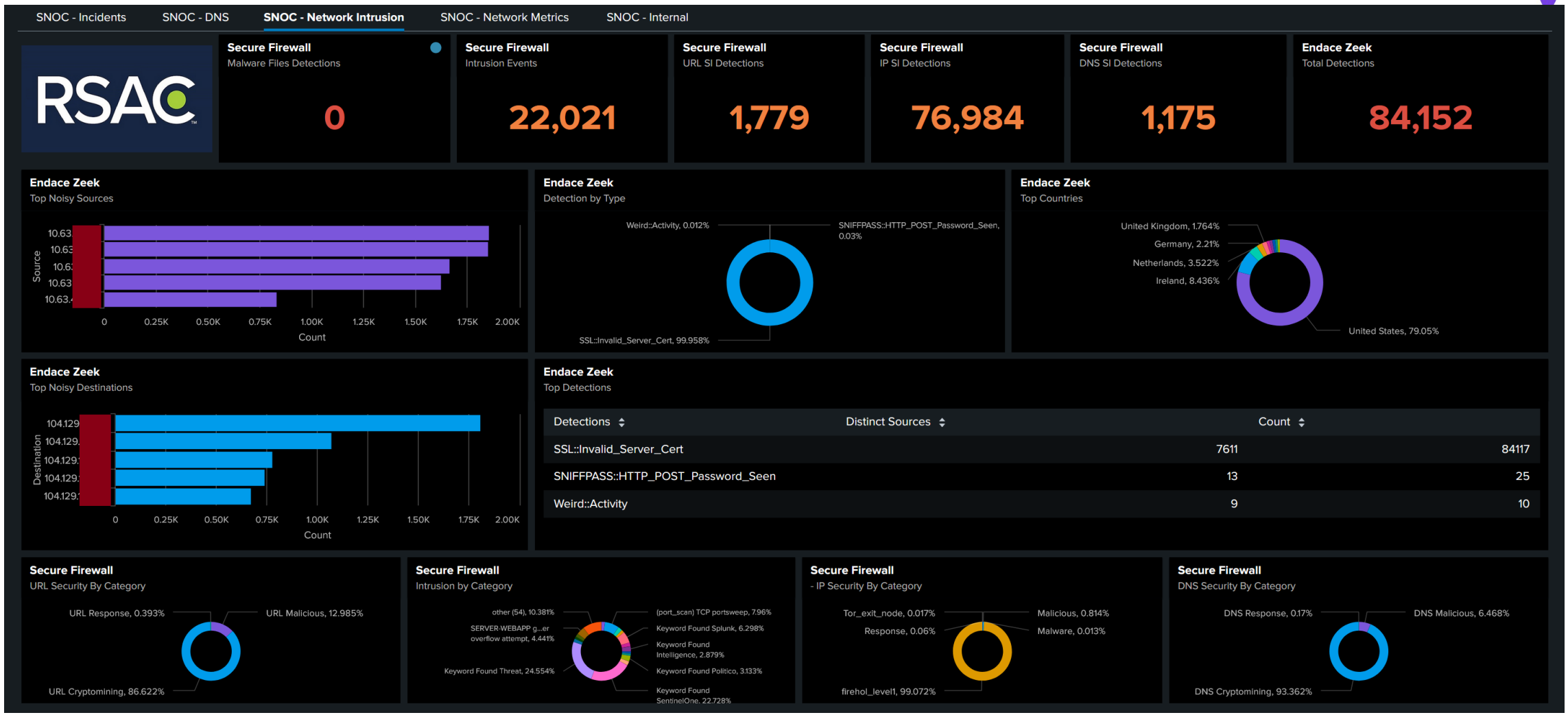
7,546 files sent to Cisco Malware Analytics for further analysis

Splunk Integrations - Incidents

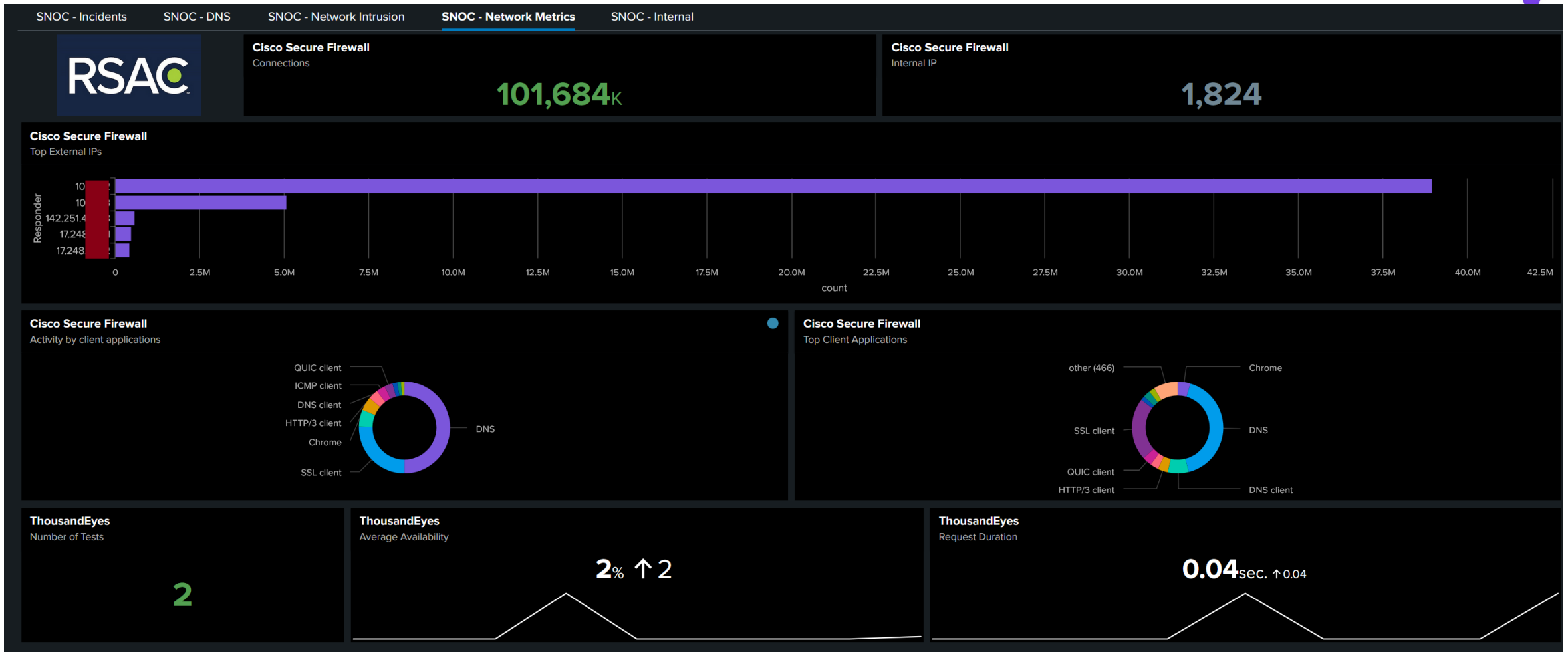
Splunk Integrations - DNS



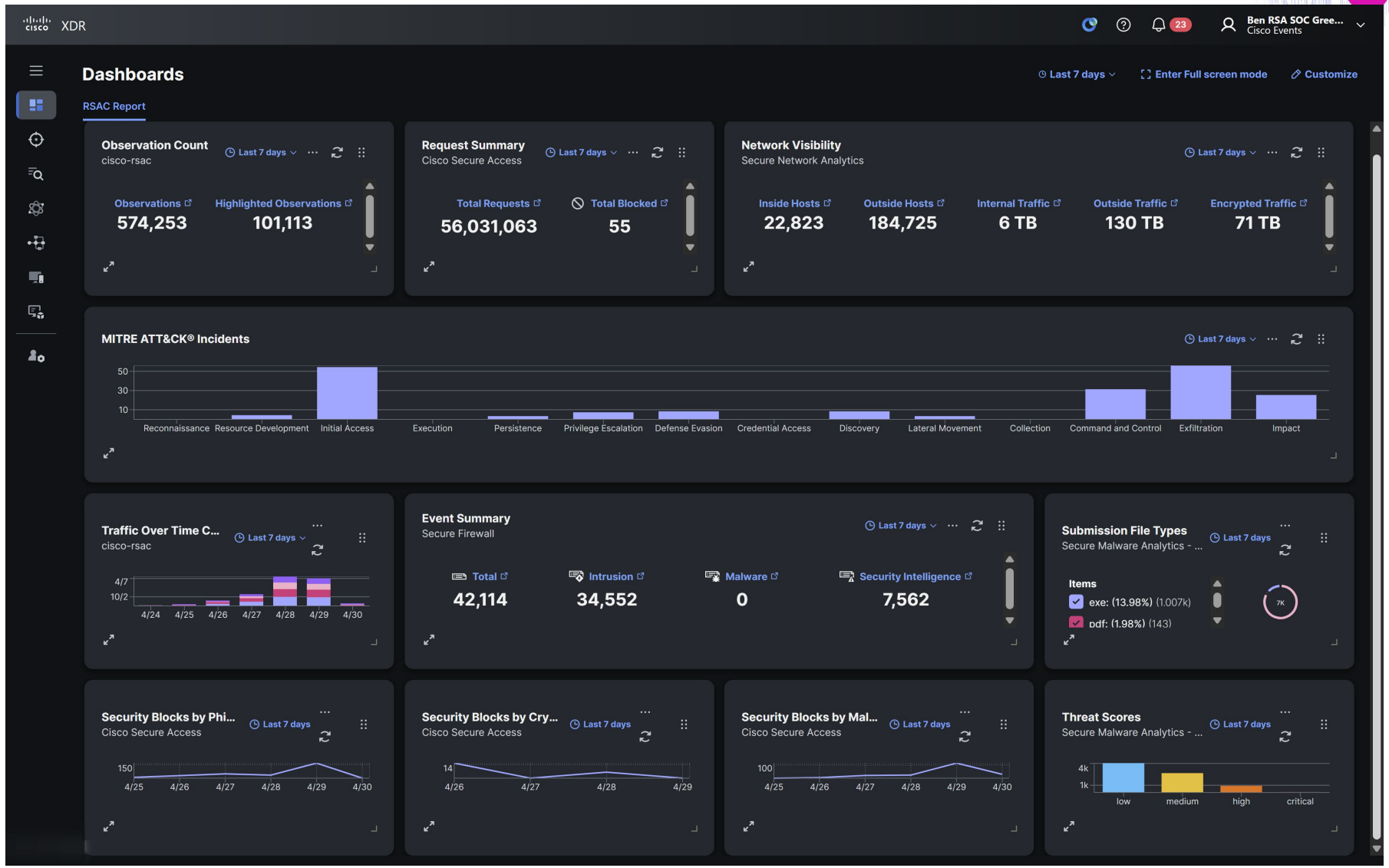
Splunk Integrations – Network Intrusion



Splunk Integrations - Network Metrics



Breach Protection - Incidents



RSAC 2025 Conference

SOC Stats

SOC Statistics

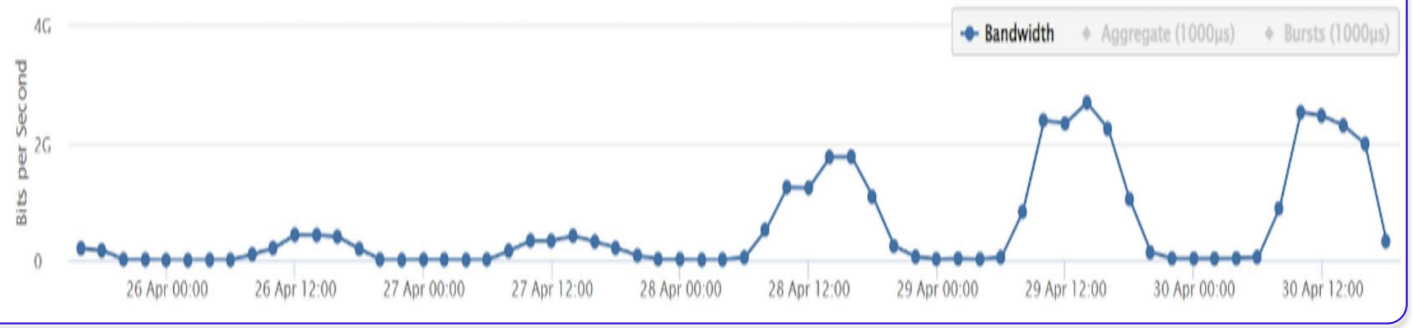
From Capture…

- Total Packets Captured: **>40 Billion** (> was 19B**)**
- Peak Bandwidth Usage: **3.4 Gbps** (> was 2.2G)
- Files Extracted **287,000** Submitted **26,374**
- Total Logs Captured: **793 million**
- Total Sessions: **615 Million** (> was 383 Million)
- **33 TB** of packet data (> was 17TB)
- **168 Gb** of log data in Splunk

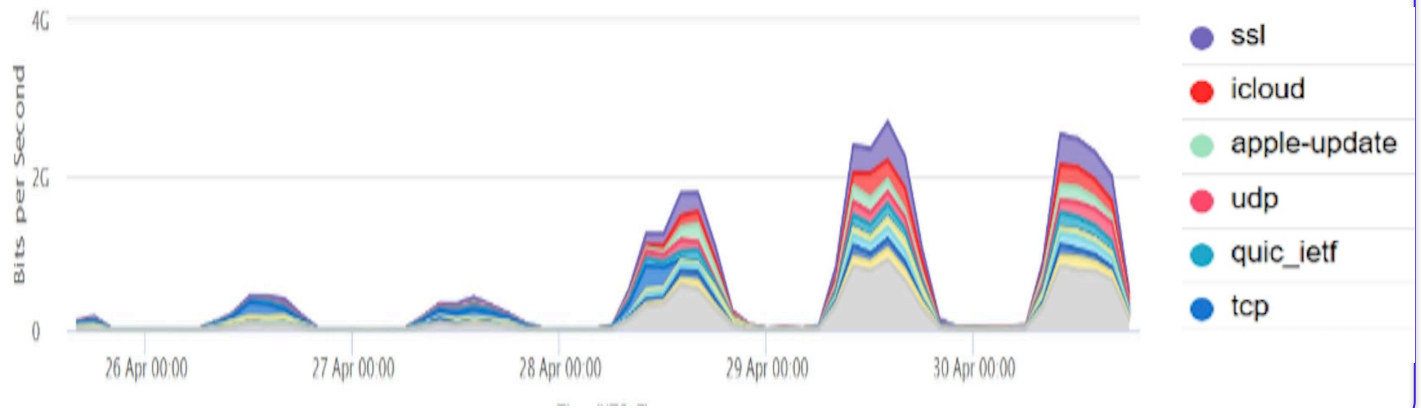
…To Detection

- Total Detection Rules: **4597 rules**
- Dedicated to this Year: **1 rule (w.w. situation)**

Network Bandwidth Trend



Application Breakdown

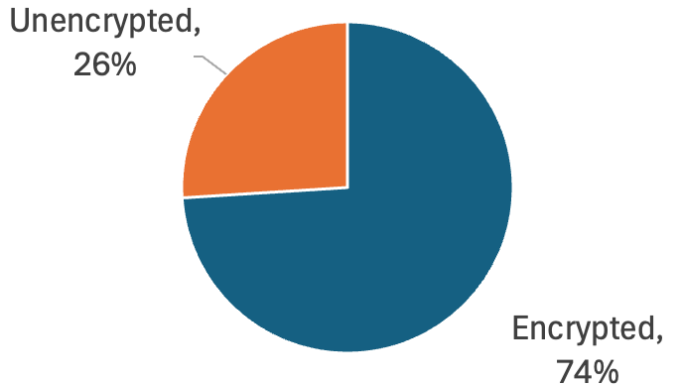


RSAC 2025 Conference

Encrypted vs Non-Encrypted: Returning to the Dark Past

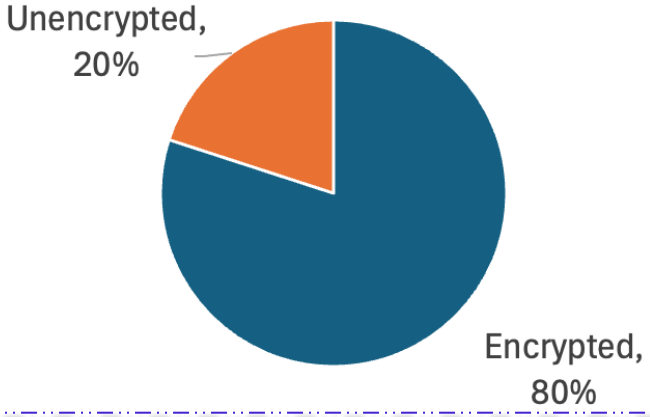
2025

The total of Encrypted Traffic: **~74%**



2024

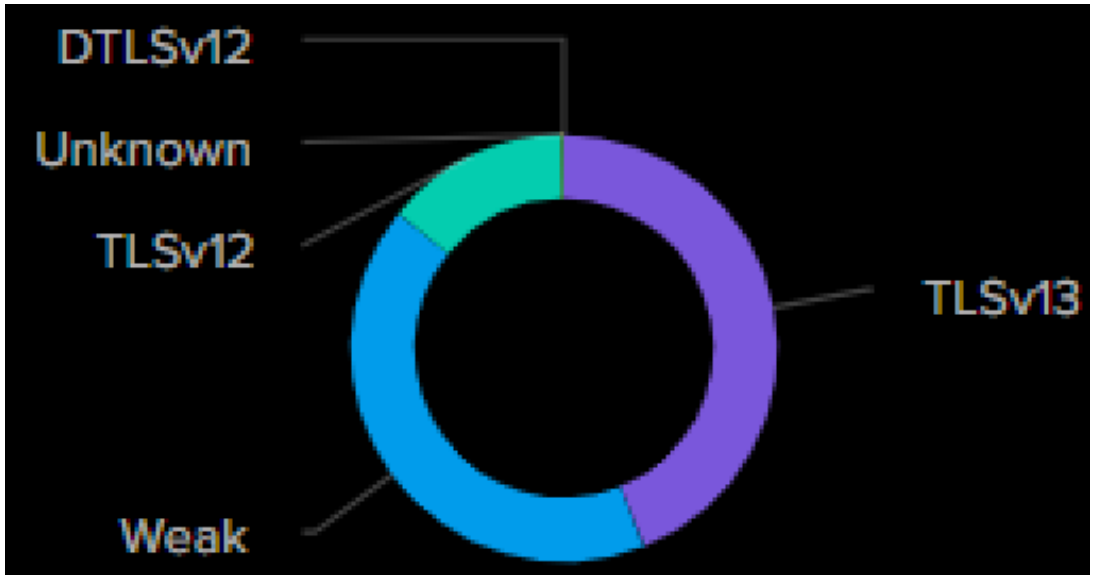
The total of Encrypted Traffic: **~80%**



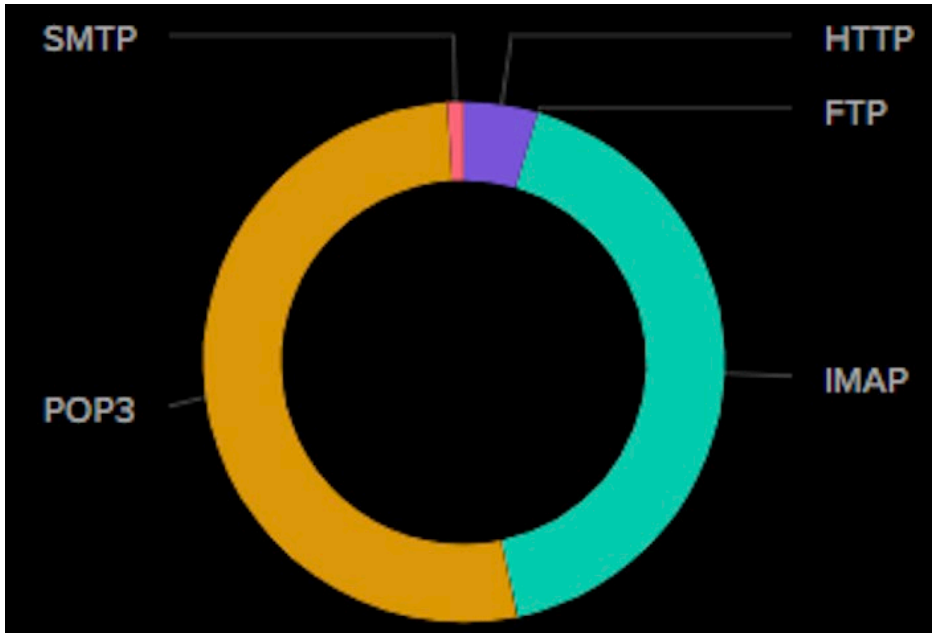
More Traffic in the clear!

Encrypted vs Non-Encrypted Expanded

Encryption Strength



Apps with Clear Text Passwords



Weak Encryption (TLS 1.0/1.1)
Increased to 40%

POP3 Refuses to DIE!
IMAP & SMTP are back.

Passwords in the Clear

2025
1,807 - Cleartext Passwords
87 - Unique Accounts (was 99)

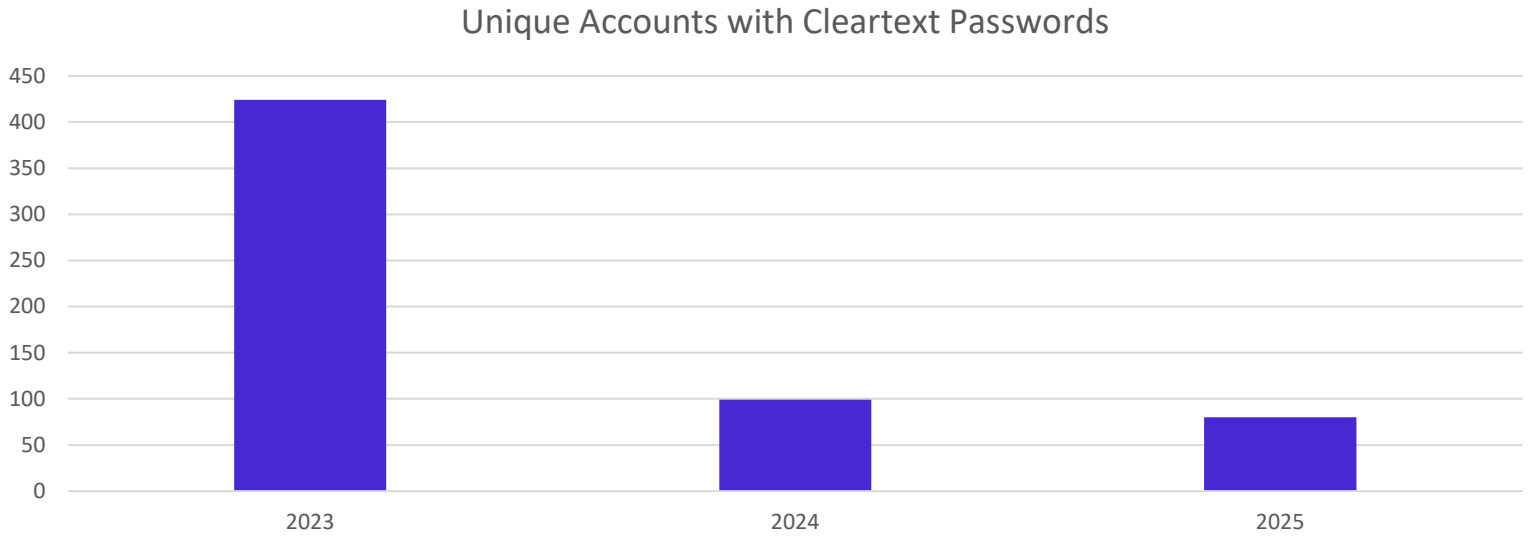
2024
20,916 - Cleartext Passwords
99 - Unique Accounts

2023
36,910 - Cleartext Passwords
424 - Unique Accounts

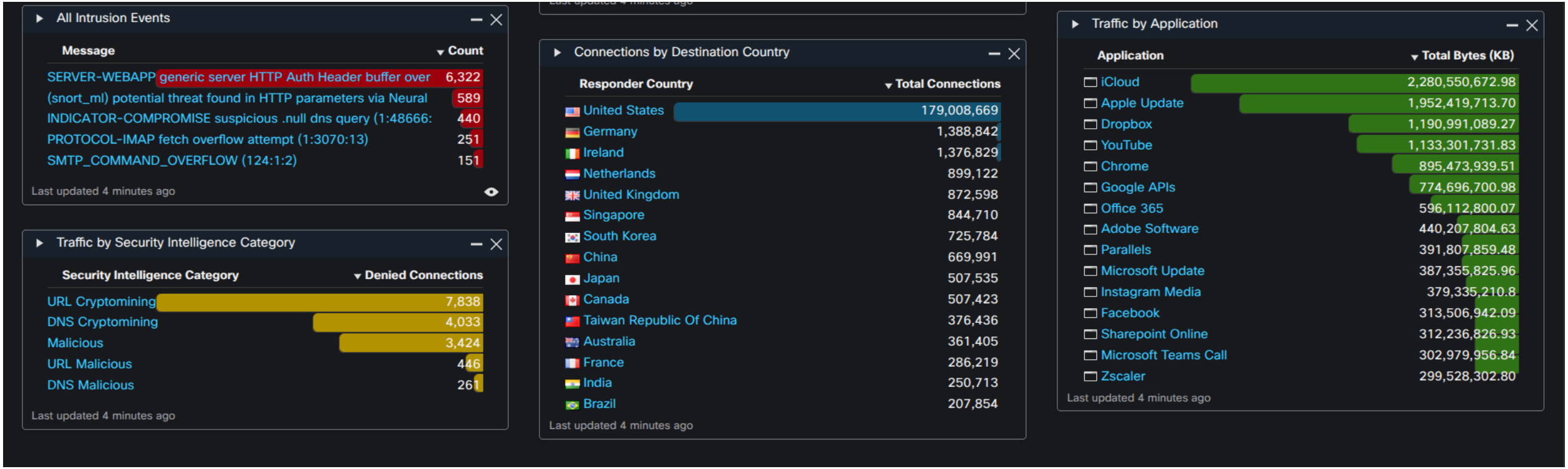
2022
55,525 - Cleartext Passwords
2,210 - Unique Accounts

2020
96,361 - Cleartext Passwords
2,178 - Unique Accounts

An Old sage once said:
«The Power of a strong password is nothing without an encrypted communication protocol!»



Geos and Downloads



All Intrusion Events

Message	Count
SERVER-WEBAPP generic server HTTP Auth Header buffer over	6,322
(snort_ml) potential threat found in HTTP parameters via Neural	589
INDICATOR-COMPROMISE suspicious .null dns query (1:48666:	440
PROTOCOL-IMAP fetch overflow attempt (1:3070:13)	251
SMTP_COMMAND_OVERFLOW (124:1:2)	151

Last updated 4 minutes ago

Traffic by Security Intelligence Category

Security Intelligence Category	Denied Connections
URL Cryptomining	7,838
DNS Cryptomining	4,033
Malicious	3,424
URL Malicious	446
DNS Malicious	261

Last updated 4 minutes ago

Connections by Destination Country

Responder Country	Total Connections
United States	179,008,669
Germany	1,388,842
Ireland	1,376,829
Netherlands	899,122
United Kingdom	872,598
Singapore	844,710
South Korea	725,784
China	669,991
Japan	507,535
Canada	507,423
Taiwan Republic Of China	376,436
Australia	361,405
France	286,219
India	250,713
Brazil	207,854

Last updated 4 minutes ago

Traffic by Application

Application	Total Bytes (KB)
iCloud	2,280,550,672.98
Apple Update	1,952,419,713.70
Dropbox	1,190,991,089.27
YouTube	1,133,301,731.83
Chrome	895,473,939.51
Google APIs	774,696,700.98
Office 365	596,112,800.07
Adobe Software	440,207,804.63
Parallels	391,807,859.48
Microsoft Update	387,355,825.96
Instagram Media	379,335,210.8
Facebook	313,506,942.09
Sharepoint Online	312,236,826.93
Microsoft Teams Call	302,979,956.84
Zscaler	299,528,302.80

Last updated 4 minutes ago

Awards – DNS Queries

#1 25: Apple | 24: Apple |23: Google

#1 25: Mchat | 24: Mchat |23: Mchat

#1 ₿⛏ 25: worldcoin | 24: IBS.Team | 23: Forsts

#1 ❤️🔥 25: grindr | 24: grindr | 23: grindr

#1 25: Cursor | 24: Notion AI

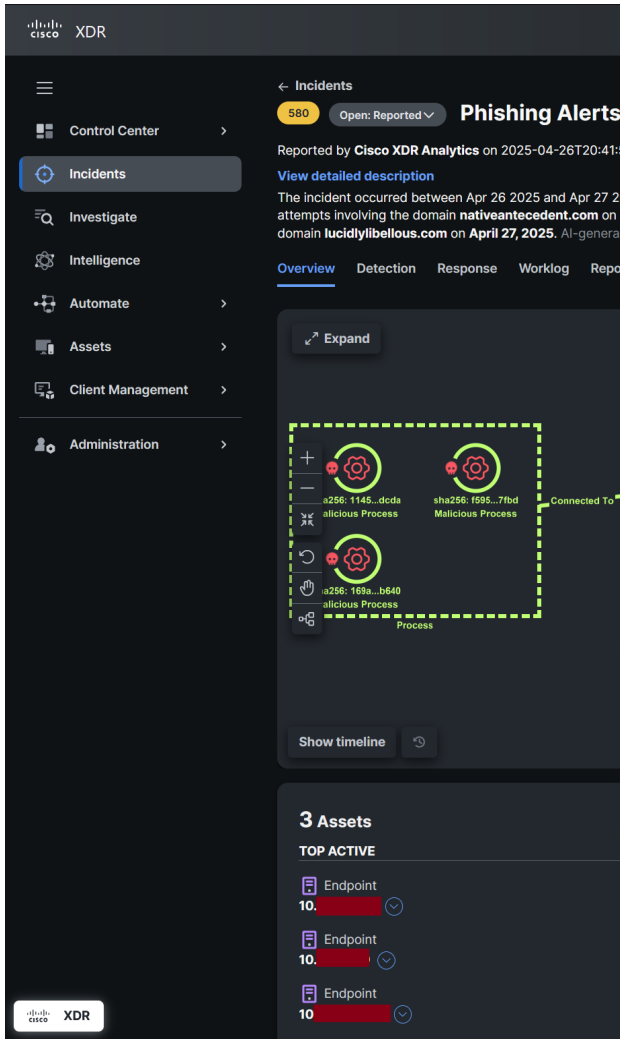
RSAC 2025 Conference

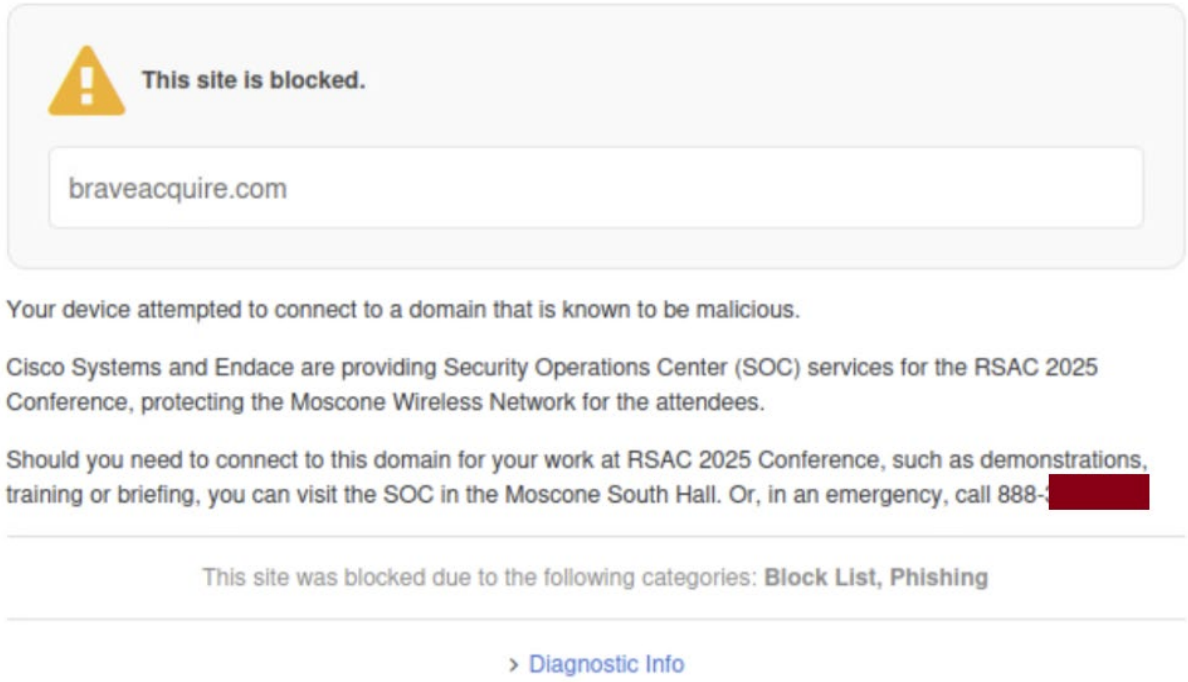
Story Time

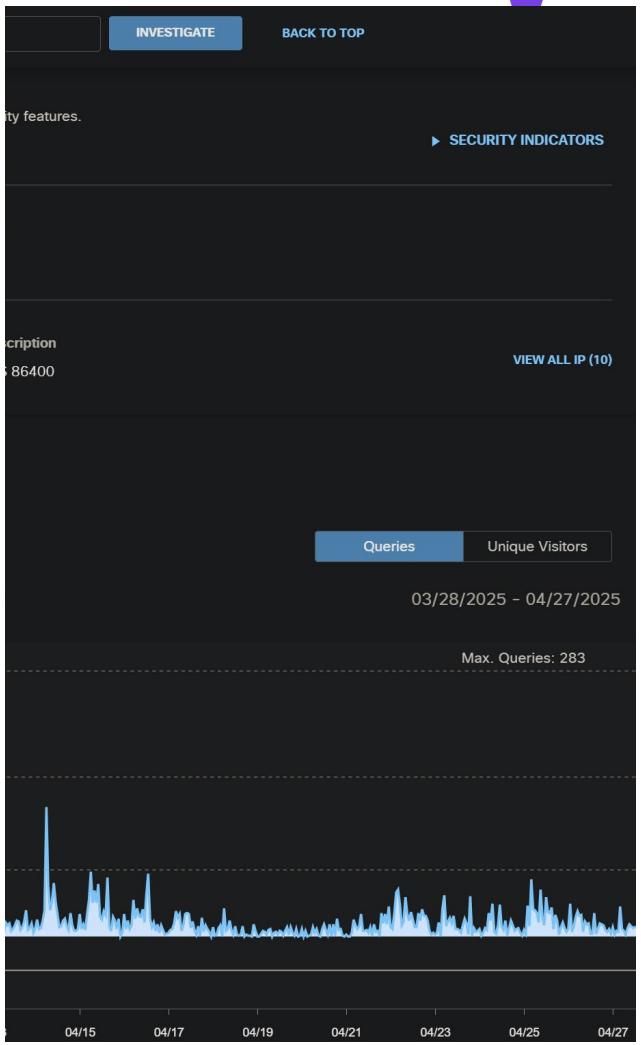
Identities Redacted

Many Voices.
One Community.

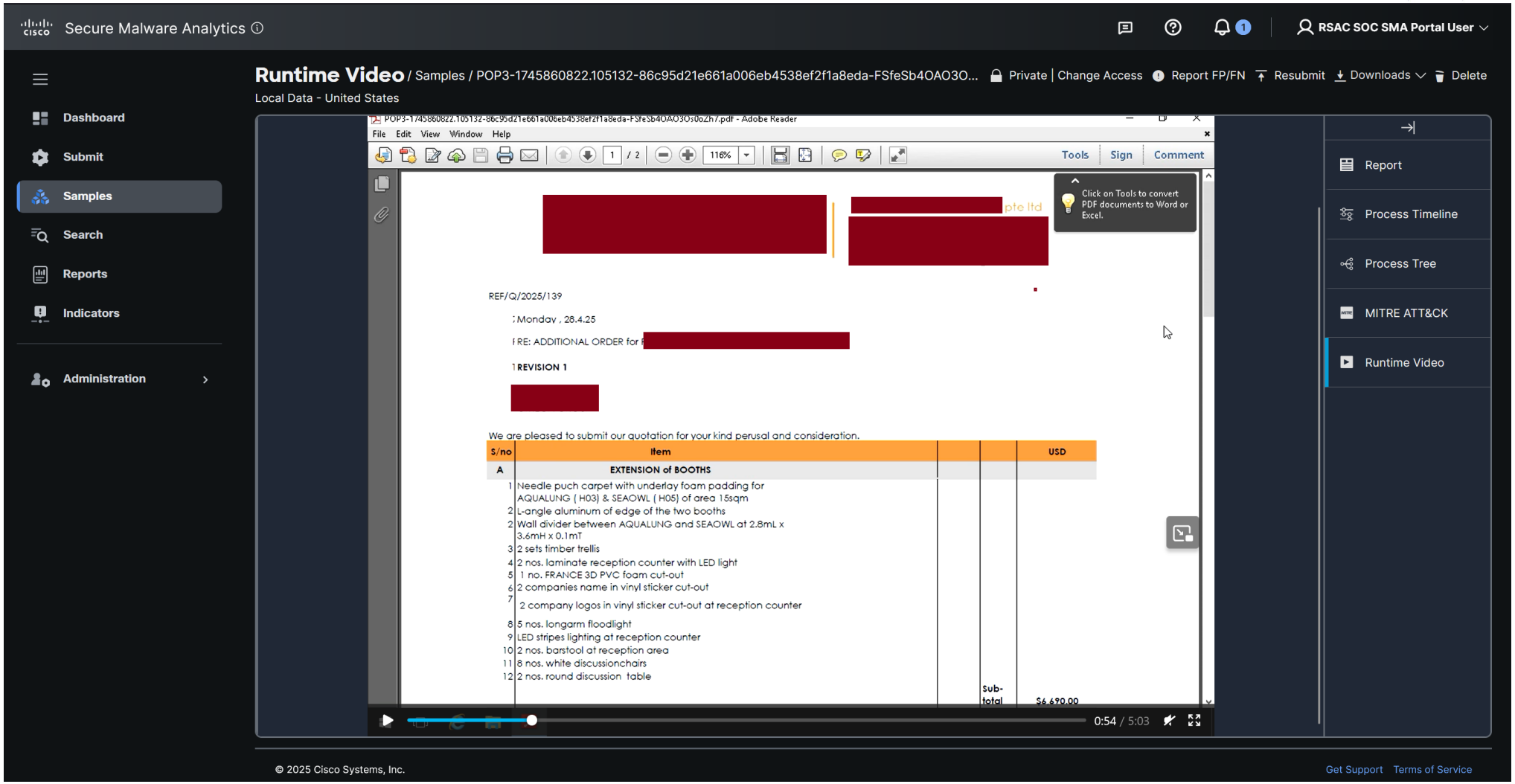
The New DGA...2 or 3 Random Words



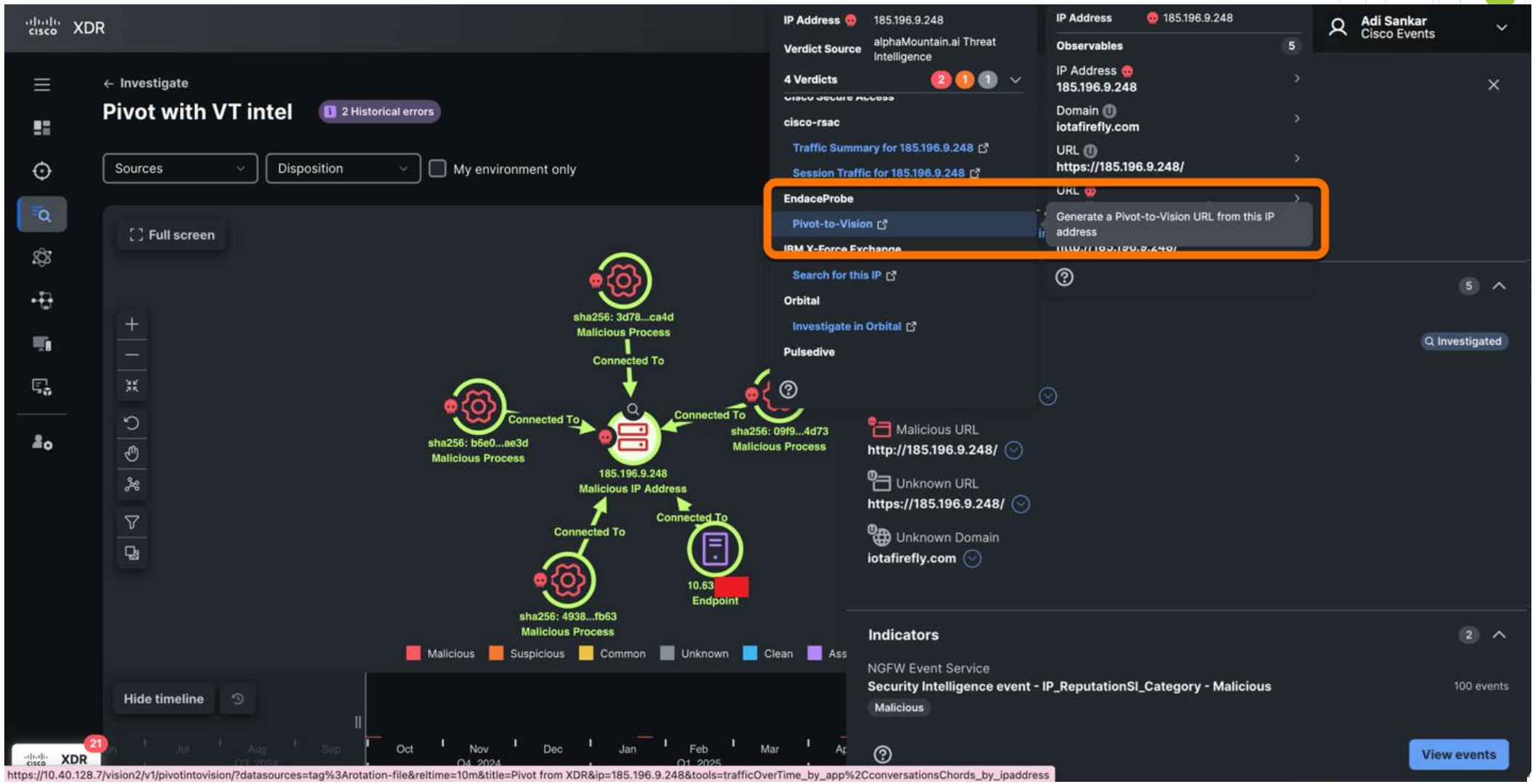

This site is blocked.
braveacquire.com
Your device attempted to connect to a domain that is known to be malicious.
Cisco Systems and Endace are providing Security Operations Center (SOC) services for the RSAC 2025 Conference, protecting the Moscone Wireless Network for the attendees.
Should you need to connect to this domain for your work at RSAC 2025 Conference, such as demonstrations, training or briefing, you can visit the SOC in the Moscone South Hall. Or, in an emergency, call 888-
This site was blocked due to the following categories: Block List, Phishing
Diagnostic Info



POP3 & SMTP (non-S) Refuse to Die


Secure Malware Analytics
RSAC SOC SMA Portal User
Runtime Video / Samples / POP3-1745860822.105132-86c95d21e661a006eb4538ef2f1a8eda-FSfeSb4OAO3O...
Private | Change Access
Report FP/FN
Resubmit
Downloads
Delete
Local Data - United States
Dashboard
Submit
Samples
Search
Reports
Indicators
Administration
Report
Process Timeline
Process Tree
MITRE ATT&CK
Runtime Video
Click on Tools to convert PDF documents to Word or Excel.
REF/Q/2025/139
Monday , 28.4.25
RE: ADDITIONAL ORDER for
REVISION 1
We are pleased to submit our quotation for your kind perusal and consideration.
S/no
Item
USD
EXTENSION of BOOTHS
Needle puch carpet with underlay foam padding for AQUALUNG (H03) & SEAOWL (H05) of area 15sqm
L-angle aluminum of edge of the two booths
Wall divider between AQUALUNG and SEAOWL at 2.8mL x 3.6mH x 0.1mT
2 sets timber trellis
2 nos. laminate reception counter with LED light
1 no. FRANCE 3D PVC foam cut-out
2 companies name in vinyl sticker cut-out
2 company logos in vinyl sticker cut-out at reception counter
5 nos. longarm floodlight
LED stripes lighting at reception counter
2 nos. barstool at reception area
8 nos. white discussionchairs
2 nos. round discussion table
Sub-total
$6,690.00
0:54 / 5:03
© 2025 Cisco Systems, Inc.
Get Support
Terms of Service

Command and Control



CnC PCAP

rsa-invmgr 0 soc — Investigations — Management

Wireshark | Pivot from XDR — Wireshark Profile | Download Saved Files | Previous 100 MB | Next 100 MB

File Edit View Go Capture Analyze Statistics Telephony Tools Help

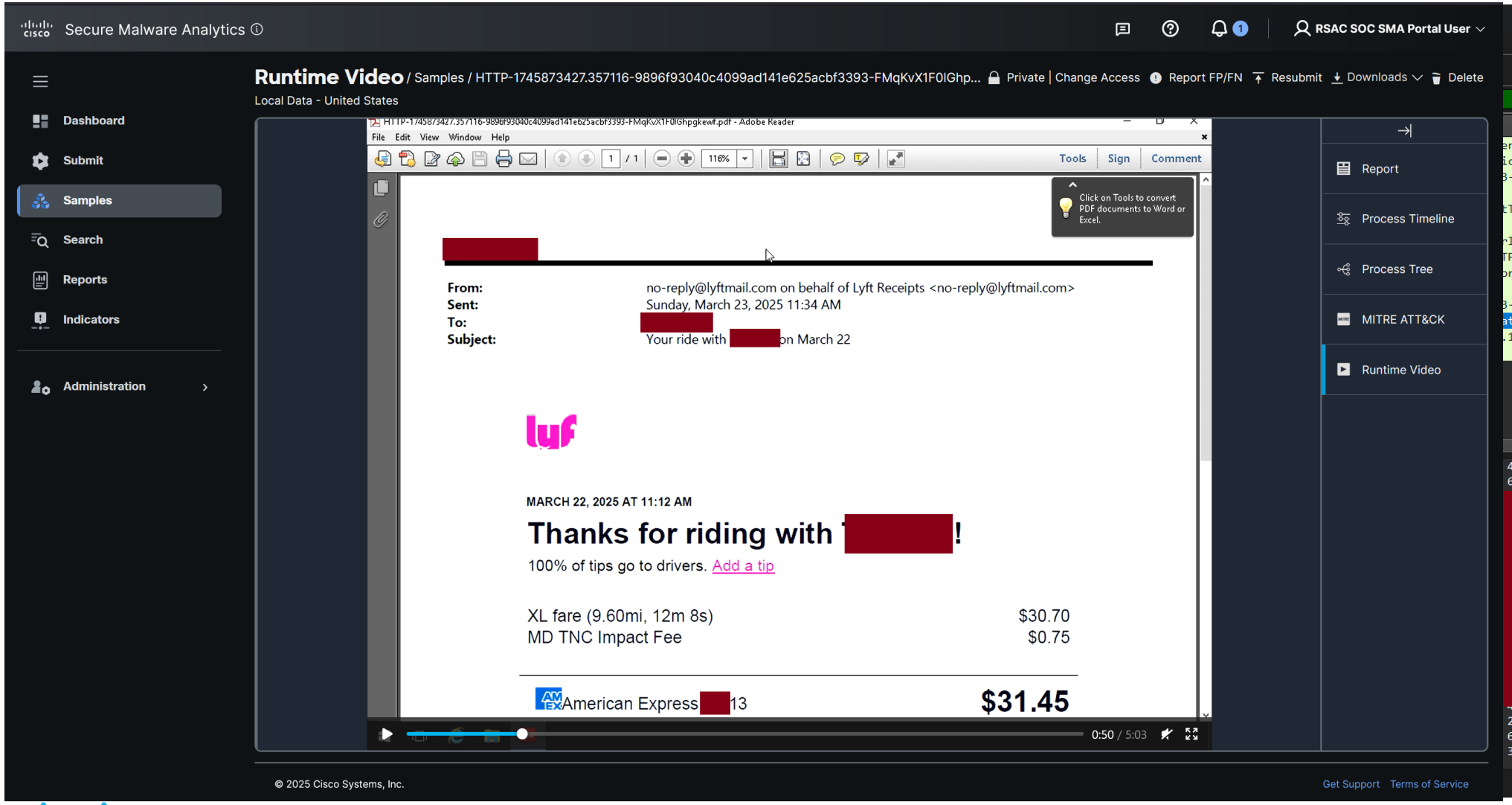
!(erf.types.type == "META")

No.	Time	Source	Destination	Protocol	Length	Info
7285	2025-04-29 11:16:03.7814661…	10.63	185.196.9.248	TCP	64	53274 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
7286	2025-04-29 11:16:03.7814665…	10.63	185.196.9.248	TCP	64	[TCP Dup ACK 7285#1] 53274 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
7287	2025-04-29 11:16:03.9392313…	185.196.9.248	10.63.	TCP	64	3912 → 53274 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0
7288	2025-04-29 11:16:04.9479789…	10.63	185.196.9.248	TCP	70	53276 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7289	2025-04-29 11:16:05.1055555…	185.196.9.248	10.63	TCP	70	3912 → 53276 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
7290	2025-04-29 11:16:05.1071251…	10.63	185.196.9.248	TCP	64	53276 → 3912 [ACK] Seq=1 Ack=1 Win=131584 Len=0
7291	2025-04-29 11:16:05.1144963…	10.63	185.196.9.248	TLSv1.3	224	Client Hello
7292	2025-04-29 11:16:05.1436230…	10.63	185.196.9.248	TCP	70	53329 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7293	2025-04-29 11:16:05.2765036…	185.196.9.248	10.63.	TLSv1.3	186	Server Hello
7294	2025-04-29 11:16:05.3011093…	185.196.9.248	10.63	TCP	70	3912 → 53329 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
7295	2025-04-29 11:16:05.3032660…	10.63	185.196.9.248	TCP	64	53329 → 3912 [ACK] Seq=1 Ack=1 Win=131584 Len=0
7296	2025-04-29 11:16:05.3058359…	10.63	185.196.9.248	TLSv1.3	224	Client Hello
7297	2025-04-29 11:16:05.3312273…	10.63	185.196.9.248	TCP	64	53276 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
7298	2025-04-29 11:16:05.4675386…	185.196.9.248	10.63.	TLSv1.3	186	Server Hello
7299	2025-04-29 11:16:05.4889965…	185.196.9.248	10.63.	TCP	64	3912 → 53276 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0
7300	2025-04-29 11:16:05.5224879…	10.63.	185.196.9.248	TCP	64	53329 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
7301	2025-04-29 11:16:05.6801091…	185.196.9.248	10.63	TCP	64	3912 → 53329 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0
7302	2025-04-29 11:16:09.9230367…	10.63	185.196.9.248	TCP	70	53334 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7303	2025-04-29 11:16:10.0805892…	185.196.9.248	10.63	TCP	70	3912 → 53334 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
7304	2025-04-29 11:16:10.0851279…	10.63	185.196.9.248	TCP	64	53334 → 3912 [ACK] Seq=1 Ack=1 Win=131584 Len=0
7305	2025-04-29 11:16:10.0905054…	10.63	185.196.9.248	TLSv1.3	224	Client Hello
7306	2025-04-29 11:16:10.2523160…	185.196.9.248	10.63	TLSv1.3	186	Server Hello
7307	2025-04-29 11:16:10.3124168…	10.63	185.196.9.248	TCP	64	53334 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
7308	2025-04-29 11:16:10.4700303…	185.196.9.248	10.63	TCP	64	3912 → 53334 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0
7309	2025-04-29 11:16:11.1196384…	10.63	185.196.9.248	TCP	70	53283 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7310	2025-04-29 11:16:11.2771142…	185.196.9.248	10.63	TCP	70	3912 → 53283 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM

```
▸ Frame 7354: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface Port A (ERF Host ac1f6b
▸ Extensible Record Format
▸ Ethernet II, Src: Intel_ed:d5:ff (3c:21:9c:ed:d5:ff), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
▸ Internet Protocol Version 4, Src: 10.63.  Dst: 185.196.9.248
▸ Transmission Control Protocol, Src Port: 53337, Dst Port: 3912, Seq: 167, Ack: 129, Len: 0
```

```
0000  00 00 5e 00 01 01 3c 21  9c ed d5 ff 08 00 45 80   ··^···<! ·····E·
0010  00 28 fb 8e 40 00 80 06  fa 95 0a 3f 36 30 b9 c4   ·(··@··· ···?60··
0020  09 f8 d0 59 0f 48 cf a6  eb a9 09 df 34 ca 50 10   ···Y·H·· ····4·P·
0030  02 01 d0 0c 00 00 00 00  00 00 00 00 8f 68 3d e0   ········ ·····h=·
```

Riding in the Clear


Secure Malware Analytics
RSAC SOC SMA Portal User
Runtime Video / Samples / HTTP-1745873427.357116-9896f93040c4099ad141e625acbf3393-FMqKvX1F0lGhp... Private | Change Access Report FP/FN Resubmit Downloads Delete
Local Data - United States
Dashboard
Submit
Samples
Search
Reports
Indicators
Administration
Report
Process Timeline
Process Tree
MITRE ATT&CK
Runtime Video
From: no-reply@lyftmail.com on behalf of Lyft Receipts <no-reply@lyftmail.com>
Sent: Sunday, March 23, 2025 11:34 AM
To:
Subject: Your ride with on March 22
MARCH 22, 2025 AT 11:12 AM
Thanks for riding with !
100% of tips go to drivers. Add a tip
XL fare (9.60mi, 12m 8s) $30.70
MD TNC Impact Fee $0.75
American Express 13 $31.45
© 2025 Cisco Systems, Inc.
Get Support Terms of Service

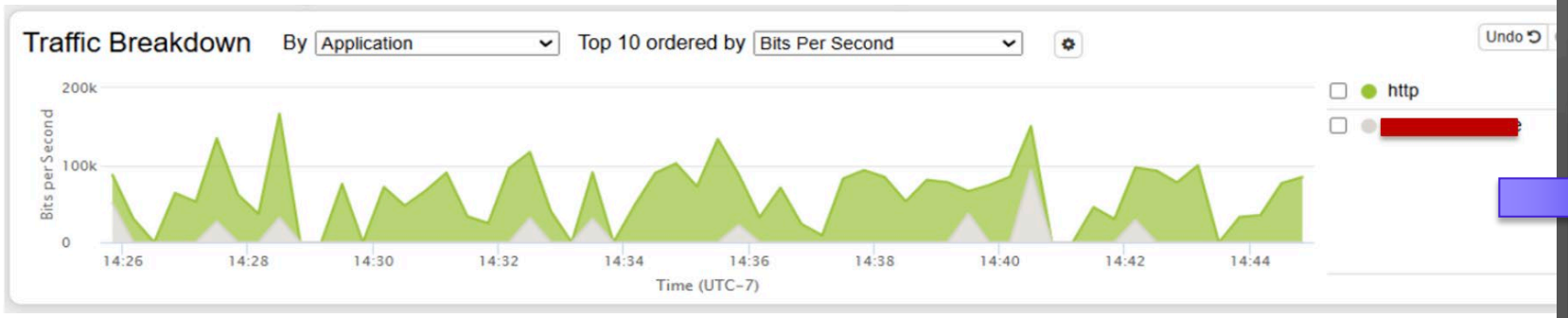
Security Through Obscurity?

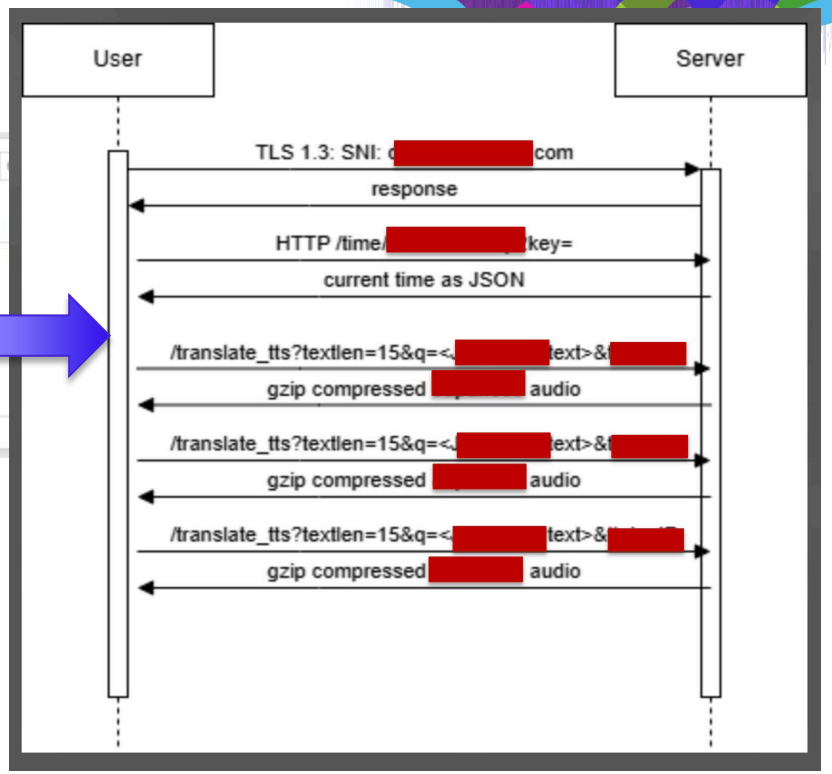
http.request.method==POST

No.	Time	Source	Destination	Protocol	Length	Info
158	65.538188	10.63	44.200.	HTTP	782	POST /login.os H
263	66.160773	10.63	44.200.	HTTP	640	POST /menu/sideb
268	66.192291	10.63	44.200.	HTTP	671	POST /request/fp
305	66.349303	10.63	44.200.	HTTP	590	POST /request/ch
406	485.308765	10.63	44.200.	HTTP	1479	POST /approval/a
457	523.275528	10.63	44.200.	HTTP	626	POST /menu/sideb
460	523.294049	10.63	44.200.	HTTP	1479	POST /approval/a
521	544.867178	10.63	44.200.	HTTP	626	POST /menu/sideb
648	1984.659056	10.63	44.200.	HTTP	626	POST /menu/sideb
660	1984.742191	10.63	44.200.	HTTP	1479	POST /approval/a
761	2049.938861	10.63	44.200.	HTTP	626	POST /menu/sideb
777	2050.021330	10.63	44.200.	HTTP	1479	POST /approval/a

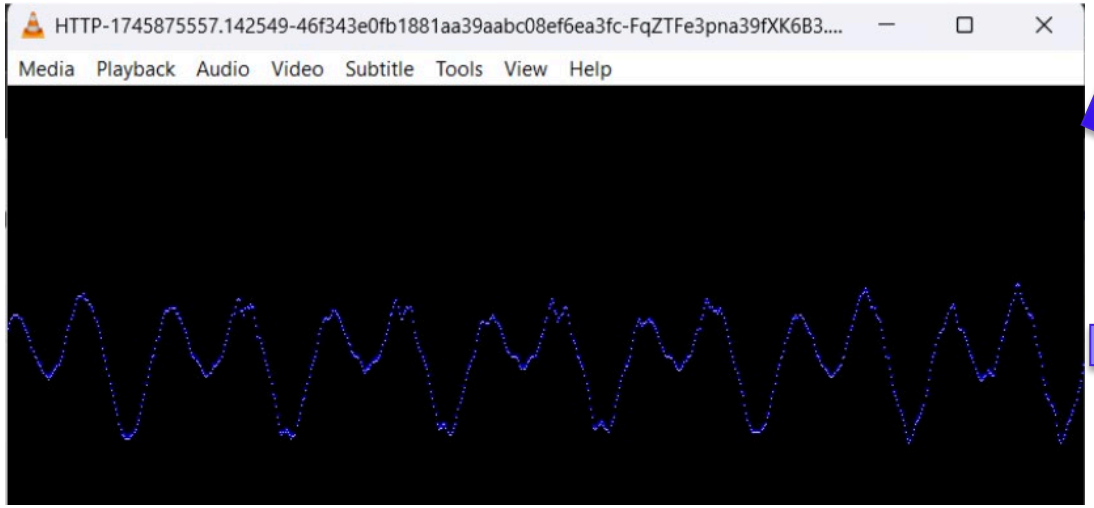
```
▸ Frame 158: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits)
▸ Ethernet II, Src: EFMNetworks , Dst: IE
▸ Internet Protocol Version 4, Src: 10.63 , Dst: 44.200.
▸ Transmission Control Protocol, Src Port: 50059, Dst Port: 8190, Seq: 2037, Ack: 949, Len: 724
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www
  ▸ Form item:
  ▸ Form item: "password" = "admin"
```

Lost in Translation





Translation Service Text & Audio in the clear



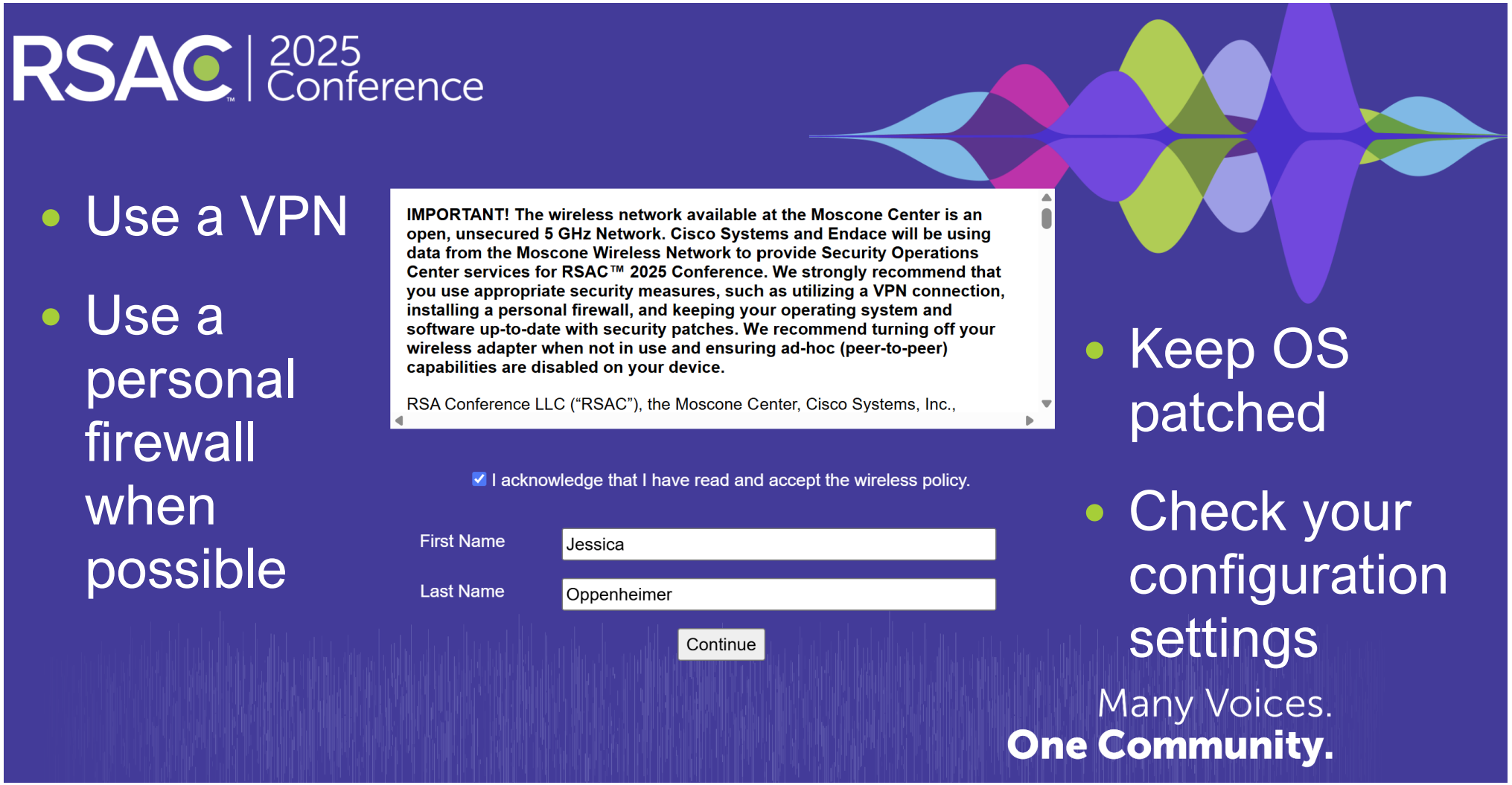
Translation: *The communication method uses buildings to move data to different locations. Defense team ….*

RSAC 2025 Conference

CCTV for Me

“Apply” Slide

- Use a VPN
- Use a personal firewall when possible


IMPORTANT! The wireless network available at the Moscone Center is an open, unsecured 5 GHz Network. Cisco Systems and Endace will be using data from the Moscone Wireless Network to provide Security Operations Center services for RSAC™ 2025 Conference. We strongly recommend that you use appropriate security measures, such as utilizing a VPN connection, installing a personal firewall, and keeping your operating system and software up-to-date with security patches. We recommend turning off your wireless adapter when not in use and ensuring ad-hoc (peer-to-peer) capabilities are disabled on your device.
RSA Conference LLC (“RSAC”), the Moscone Center, Cisco Systems, Inc.,
I acknowledge that I have read and accept the wireless policy.
First Name
Jessica
Last Name
Oppenheimer
Continue

- Keep OS patched
- Check your configuration settings

Many Voices.
One Community.

RSAC™ 2025 Conference

Many Voices.
One Community.